Pūraitė Aurelija,
Associate Professor,
Mykolas Romeris University,
Academy of Public Security,
Lithuania, Kaunas
e-mail: aurelija.puraite@gmail.com

Šilinskė Neringa,
Doctoral student,
Turiba University, Faculty of Law,
Latvia, Ryga,
e-mail: n.silinske@gmail.com

doi: 10.21564/2414–990x.144.157226
UDC 341.232.7

IMAGE CAPTURING DEVICES: THREAT OR GOOD?

The authors of the paper 'weight' advantages and threat to privacy caused by the usage of unmanned aerial vehicles (drones) and dashboard cameras. By analysing and comparing legal regulation of two gerographically, historically and culturally close countries (Latvia and Lithuania) they indicate differences of regulation of privacy, problematic aspects of their current national regulation on the usage of technologies in-topic and privacy protection and suggest possible solutions to the legal shortcomings found.

Keywords: unmanned aerial vehicles; drones; dashboard camera; privacy; Latvia; Lithuania.

Пурайте А., доцент, факультет громадської безпеки, Університет Миколаса Ромеріса, Литовська Республіка, м. Каунас.
e-mail : aurelija.puraite@gmail.com

Сілінску Н., аспірантка, факультет права, Університет Туріба, Латвія, м. Рига.
e-mail : n.silinske@gmail.com

Прилади, що фіксують зображення: загроза чи благо?

Автори статті «зважили» переваги та загрози втручання у приватне життя, що виникають внаслідок використанням безпілотних літальних апаратів (дронів) і відеореєстратора. Аналізуючи та порівнюючи законодавство двох географічно, історично та культурно близьких країн – Латвії та Литви, вони вказують на відмінності в законодавчому врегулюванні питань конфіденційності, проблемні аспекти їх чинного національного законодавства щодо використання технологій та захисту приватного життя, а також пропонують можливі рішення щодо врегулювання виявлених правових прогалин.

Порівняння двох законодавств, які регулюють однакові питання конфіденційності та використання камер UAS та панелі приладів, засвідчує, що національне законодавство, навіть відповідно до одного – законодавства Європейського Союзу – може захистити таку саму цінність різними правовими інструментами. Кожне законодавство – литовське та латвійське – має свої переваги та недоліки, але можна підтвердити, що закон не завжди йде в ногу з швидким розвитком технологій. Як було показано, з особливими коригуваннями щодо ідентифікації користувачів камер UAS та панелі приладів, з упровадженням правових інструментів, що дозволяють потерпілій стороні ефективно захищати власність у випадках, коли користувачі персональної інформації є особами, що збирають особисту інформацію не в комерційних цілях, можна знайти правильний баланс між цими двома цінностями – соціальною безпекою та власністю.

Переваги нових технологій не можна було заперечувати, тому було б безглуздо говорити, що вони не є необхідними, оскільки викликають велику небезпеку для нашої власності. Власність як цінність не може бути абсолютною. Тому важливо адаптувати правові механізми до мінливих загроз основним цінностям, таким як власність. Таким чином, відсутність правових заходів не може бути підставою для втручання в технологічний розвиток: не слід розглядати нові технології як загрозу, а правові норми повинні бути вдосконалені і пристосовані до постійно мінливого світу.

Ключові слова: безпілотні літальні апарати; дрони; відеореєстратори; власність; Латвія; Литовська Республіка.

Introduction. Lithuanians have a saying that instead of hearing a hundred times it is better to see once. Such saying confirms that visual means convey most of the information. Thus, it could be said that filming devices are the best tool to collect the most accurate information. However, along with the development of image capturing devices and other technologies, people's concern about their privacy grows. And this could be confirmed by the General Data Protection Regulation (hereinafter – GDPR)[1] which came into force just recently. The fact that the necessity of such regulation was noticed by the European Union proves that people's private information as a part of their right to private life, had been in danger. The same, confirming the **novelty and actuality of the topic**, is stated in the preamble of the GDPR: «*Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities.*»[2] Adding to the latter, the GDPR does not apply to the processing of personal data by a natural person in the course of a purely personal

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *OJ L 119, 4.5.2016, p. 1–88.*

[2] Ibid: preamble point 6.

or household activity and thus with no connection to a professional or commercial activity,[1] but technologies serve not only private companies and public authorities, but also natural persons in collecting of personal data for various purposes, including illegal ones.

On the other hand, the image capturing devices give people immense opportunities and to be able to enjoy them it is worth working on the adjustment of current legislation in order **to find the right balance** between the value given by the technologies in-topic (security) and the other value that is so much in-danger nowadays (privacy). The latter forms **the research problem**. So in this **research the answer** on how the current legal regulation could be adjusted in order to find that balance, is given.

By **comparing and indicating** the problematic aspects of current national Latvian and Lithuanian regulation on the usage of technologies in-topic and privacy protection, the authors aim to prove that even though the regulation on protection of particular values could differ in different jurisdictions or even be insufficient, the image capturing devices still make a great contribution to societal security therefore their use cannot be denied. In order to adjust their impact on privacy, prevent, tackle breaches of privacy, it is necessary to suggest the correction of legal rules.

1. Image capturing devices and their contribution to societal security

1.1. Justification of the choice of particular image capturing devices

There exist many image capturing devices. But two types of them are very specific – unmanned aerial systems (hereinafter – UAS) and dashboard cameras (cameras mounted in cars/car cameras). These devices have some things incommon: they both are mainly used to capture images (videos) and they are moving, therefore it allows their operators to remain unidentified and in such way to avoid liability. UAS and dashboard cameras are specifically chosen as a research object because their use is widespread and at the same time very specific: for example, video surveillance can be carried out secrectly – when the filmed person does not even realise he/she is being filmed. Also, the UAS can capture videos of the places that could not be achieved easily (for example, private, closed, fenced yards or premises), dashboard cameras, if not specially marked, could be imperceptible but at the same time collecting a lot of information and very often the object observed cannot even choose whether to allow such observation or not (for example, working dashboard camera in a traffic flow or an object could be secretly monitored if a car with a dashboard camera on was left in some area)[2]. Such characteristics make the two devices more specific and worth deeper analysis and because images convey most of the information and peoples' right to privacy could be easily breached by video capture, possession and distribution, these two technologies, as the most threatening the privacy, are chosen as an object of this article.

[1] Ibid: preamble point18.

[2] Bučiūnas, G. (2015). Vaizdo registratoriai ir asmens privatumas, *Mokslo taikomieji tyrimai Lietuvos kolegijose,* Vol. 1, No. 11: 65.

1.2. Image capturing devices and their relation to societal security

The understanding of security has been changing all the time. If in the XVII'th century, when the Treaty of Westphalia was signed, security was understood as a peaceful settlement of disputes among the states,[1] nowadays, when people seek for more comfortable living, use more technologies, such as UAS, dashboard cameras, which have overtaken a part of our privacy, without the traditional security perception, new forms of security have evolved.[2]

According to the European Union open data, economic and financial matters are one of the biggest challenges to the security of European Union citizens, after terrorism.[3] Therefore it could be said that the economic wellfare is one of the most important elements of people's security. As it will be seen later, the image capturing devices make a great positive influence on economy, whereas economy is one of the areas related to pepople's security. Furthermore, it could not be denied that one of the most important factors determining people's sence of security is their physical safety from various threats (crimes, terrorism, environmental factors). Thus, the term 'societal security' is used in this article, as it encompasses not only physical safety, but general use for society and individuals, including safety assurance, economical use, people's emotional satisfaction.

Many authors have analysed the importance of technologies, such as drones and dashboards cameras and their contribution to individual and public welfare. For example, J. Villasenor[4] stresses that theres is an endless variety of civil applications that the UAS can be employed in and that overwhelming majority of them is beneficial. This author, as well as Martin McKown[5], stresses puporses that UAS could be used for: people's search and resque operations, surveying, traffic congestion monitoring, air quality assessment, wildlife tracking. As the main topic drone's use in monitoring soil residue cover is analysed by other authors[6]; A.G. Entrop and A. Vasenev[7], as well as others[8] highlight the UAS's use in construction industry,

[1] Vadapalas, V. (1998). *Tarptautinė teisė. Bendroji dalis (International Law. General Part)*, Vilnius: Eugrimas: 76.

[2] Puraite, A, Silinske, N. (2017). Understanding the concept of security: theoretical approach. *Public Security and Public Order,* Vol. 19: 136.

[3] EU Open Data Portal, „Special Eurobarometer 432: Europeans' attitudes towards security." (2015). Retrieved 25.11.2017 from http://data.europa.eu/euodp/en/data/dataset/S2085_83_2_432_ENG/resource/ae0b54bc-3974-4165-9f7d-c2907cb3f41f.

[4] Villasenor, J. (2013). Observation from above: Unmaneed Aircraft Systems and Privacy. *Harvard Journal of Law and Public Policy,* Vol 36: 459.

[5] McKown, M. (2015). The New Drone State: Suggestions for Legislatures Seeking to Limit Drone Surveillance by Government and Nongovernment Controllers, *University of Florida Journal of Law and Public Policy*, vol. 26: 76.

[6] Kavoosi, Z., Hossein Raoufat, M., Dehghaani, M., Jafari, A., Kazemeini, A., Jafar Naazemossadat, M. (2018). Feasibility of satellite and drone images for monitoring soil residue cover, *Journal of the Saudi Society of Agricultural Sciences*, „in press" version. doi: https://doi.org/10.1016/j.jssas.2018.06.001.

[7] Entrop, A.G., Vasenev, A. (2017). Infrared Drones in the Construction Industry: Designing a Protocol for Building Thermography Procedures, *Energy Procedia*, Vol. 132.

[8] Dupont, Q. F. M., Chua, D. K.H., Tashrif, A., Abbott, E. L.S. (2017). Potential Applications of UAV along the Contruction's Value Chain, *Procedia Engineering*, Vol. 182.

whereas other authors name UAS as being used to observe, analyze and evaluate the traffic flow as well as safety conditions.[1] It is also worth mentioning professional or leisure photography, recreational purposes of UAS as the most popular ways of use among regular users of UAS. Whereas as the main advantages of dashboard cameras ensurance of secure driving[2], provision of information about the details of traffic accidents, helping to avoid disputes on factual circumstances, as well as ensurance of public security, crime prevention, also taxi drivers' tool helping to ensure their security and dashboard cameras recreational purpose (for example, videos about family road trips)[3] are mentioned.

Most of the abovementioned advantages of the technologies make a great influence on economy. European Drones Outlook Study carried out by The SESAR Joint Undertaking, disclosed that the growing drone market shows significant potential: economic impact analysis of the entire value chain for each of the areas of demand revealed the potential for a European market exceeding 10 billion annually by 2035 and 15 billion annually by 2050.[4] The development of market also provides new jobs throughout all Mebmer States. It is summarized that over 100 000 jobs are estimated to be created with a market this significant.[5] Additionally, even though the forecast has been prepared on the basis of number assumptions,[6] the conclusion is that taking into consideration even more conservative assumptions, the foreseen growth is still significant.[7]

Also, unofficial sources disclose that in 2013 only 1 percent of motorists used dashboard cameras in the UK. In 2017 that figure had jumped to 15 percent. Market estimates suggest a further 30 percent of motorists plan to use one in the near future in the UK.[8]

These advantages and the ways of use of the technologies undeniably confirm that their impact on societal security is significant.

---

[1] Khan, M. A., Ectors, W., Bellemans, T., Ruichek, Y., Yasar, A. H., Janssens, D., Wets, G. (2018). Unmanned Aerial-Vehicle Based Traffic Analysis: A Case Study to Analyze Traffic Streams at Urban Roundabouts, *Procedia Computer Science*, Vol. 130.

[2] Rogavichene, L., Garmonnikov, I. (2017). Innovative Technologies for Assessment and Correction of the Driving Style, *Transportation Research Procedia*, Vol. 20.

[3] Nauwelaerts, W., World Data Protection Report: Guidelines on Use of Dashboard Cameras (2014), retrieved 06.05.2018 from https://www.hunton.com/files/Publication/a75c66a4-2f6f-4e3e-a83b-543923987393/Presentation/PublicationAttachment/580a5a0c-66f6-4cee-834c-8b41b637fd09/Guidelines_on_Use_of_Dashboard_Cameras.pdf

[4] SESAR, European Dornes Outlook Study, Retrieved 01.02.2018 from https://www.sesarju.eu/sites/default/files/documents/reports/European_Drones_Outlook_Study_2016.pdf: 29.

[5] Ibid: 29.

[6] Ibid: 2.

[7] Ibid: 29.

[8] The Telegraph, retreived 06.05.2018 from https://www.telegraph.co.uk/business/risk-insights/dashcam-benefits/.

2. Privacy and risk to breach it in the context of the use of image capturing devices

2.1. Privacy concept and its protection by relevant legal acts

The Universal Declaration of Human Rights states that no one shall be subject to arbitrary interference with his privacy, family, home and that everyone has the right to the protection of the law against such interference.[1] The right to privacy is also enshrined in the Convention for the Protection of Human Rights and Fundamental Freedoms. [2] Its Article 8(2) states that the interference by a public authority with the exercise of this right is allowed only in accordance with the law and only if necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

European Court of Human Rights in one of its decisions stated that the notion of private life should be interpreted broadly but not restrictively and that such interpretation means that personal information is any information relating to an identified or identifiable individual.[3] It proves that any information collected by image capturing devices even indirectly connected with a person which could be identified by it, is considered personal data.

Furthermore, in the European Union level the right to privacy is also protected by the Charter of Fundamental Rights of the European Union,[4] as well as regulated in the GDPR which intends to protect natural persons' personal data as a «third generation» fundamental right.

By national legal acts the right to privacy is protected at the national level. In Lithuanian legislation the right to privacy is described in various legal acts. Besides the main legal act – the Constituion, enshrining people's right to privacy[5], there is the Law on Personal Data Legal Protection of the Republic of Lithuania (hereinafter – LPDLP) which is in accordance with the GDPR and protects personal information, but does not apply to the processing of personal data by a natural person with no connection to a professional or commercial activity.[6] As the national

[1] Universal Declaration of Human Rights, 1948, Paris. Retrieved from http://www.un.org/en/universal-declaration-human-rights/: 12.

[2] Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14. 1950, ETS 5 // http://www.refworld.org/docid/3ae6b3b04.html: 8.

[3] *Amann v. Switzerland*, no. 27798/95, §65, ECHR 2000-II.

[4] Charter of Fundamental Rights of the European Union, 7.12.2000, OJ C 326, 26.10.2012, p. 391–407: 7,8.

[5] *Lietuvos Respublikos Konstitucija (Constitution of the Republic of Lithuania)*, Official Gazette (1992, no. 220, 33-1014): Art 22 states that The private life of an individual shall be inviolable. Personal correspondence, telephone conversations, telegraph messages, and other intercommunications shall be inviolable. Information concerning the private life of an individual may be collected only upon a justified court order and in accordance with the law. The law and the court shall protect individuals from arbitrary or unlawful interference in their private or family life, and from encroachment upon their honour and dignity

[6] Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas (Law on Personal Data Legal

legislation must correspond to the European union legislation, the LPDLP was changed just after the GDPR came into force so that it corrpesponded with the latter. After the newest changes, the separate article connected with video surveillance has expired therefore Lithuania does not have any special rules on video surveillance any more and does not have any special separate regulation on the usage of dashboard cameras. There is only an act governing the usage of UAS, which is called «The rules for the use of unmanned aircrafts» (hereinafter – the Rules).[1] Unfortunately, trying to find a hint about protection of privacy in the Rules will fail, as they are intended to set only physical safety requirements of the usage of UAS.[2] On the contrary to its predecessors, we will find some privacy protection rules in the Regulation EU 2018/1139, which came into force just recently.[3] The latter stresses that unmanned aircrafts present risks for privacy, protection of personal data, therefore the requirements concerning the registration of unmanned aircraft and of operators of unmanned aircraft should be laid down (also, the Regulation sets the essential requirements for registration) and that it is also necessary to establish digital, harmonised and interoperable national registration systems in which information, including the same basic data, about unmanned aircraft and operators of unmanned aircraft registered.[4]

Lithuania also has a Civil Code which establishes the inviolability of the individual's privacy and stresses that a person's private life may be made public only with that person's consent.[5] The following point of the same article concretizes what a violation of a person's private life is and lists actions, such as unlawful invasion of person's dwelling or other private premises as well as fenced private territory, observation of one's private life, unlawful search of the person or his property, etc.; and states that the given list is not finite. The regulation of the Civil code is special because the rules on privacy protection, set in it, are applied to natural persons as well and they enable the party whose legitimate interests have been violated, to take legal remedies, including requesting for the compensation. However, in order to apply civil liability, all four conditions of the civil liability, must be proved - unlaw-

Protection of the Republic of Lithuania), Official Gazette, 1996, No. 63-1479; 2000, No. 64-1924; 2003, No. 15-597; 2008, No. 22-804; TAR, 2018-07-11, No. 2018-11733: 1.

[1] *Bepiločių orlaivių naudojimo taisyklės (The rules for the use of unmanned aircrafts)*. TAR, 2014, No. 2014-00438.

[2] Puraite, A., Bereikiene D., Silinske, N. (2017). Regulation of Unmanned Aerial Systems and Related Privacy Issues in Lithuania, *Baltic Journal of Law and Politics*, Vol. 10: 118.

[3] Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 (Text with EEA relevance.), *OJ L 212, 22.8.2018, p. 1–122*.

[4] Ibid: preamble, point 31.

[5] *Lietuvos Respublikos civilinis kodeksas (Civil Code of the Republic of Lithuania)*, Official Gazette (2000), No. 74-2262; 200: 2.23.

ful actions (for example, breach of article 2.23 of the Civil Code of the Republic of Lithuania or any other legal act guaranteeing the right to privacy), causation (only damages related to unlawful actions can be compensated), fault (article 6.248(1) of the Civil Code of Republic of Lithuania states: «Civil liability shall arise only upon the existence of the fault of the obligated person, except in the cases established by laws or a contract when civil liability arises without fault») and damage.[1] Taking into consideration the specifisity of UAS and dashboard cameras, proving unlawful actions would be quite difficult, whereas proving damage – even harder. This explains why there are no civil cases of privacy defence against illegal usage of UAS and dashboard cameras in Lithuania.

Article 2.22 of the Civil Code of the Republic of Lithuania protects natural person's right to an image. Photograph (or its part) or some other image of a natural person may be reproduced, sold, demonstrated, published and the person may be photographed only with his/her consent. However, the consent shall not be required if such acts are related to person's public activities, his official post, request of law enforcement agencies or where a person is photographed in public places, but are not allowed to be demonstrated, reproduced or sold only if those acts were to abase person's honour, dignity or damage his professional reputation.[2] This article is closely related to the usage of UAS and dashboard cameras as person's image is the best source of his identification therefore is one of the components of the right to privacy. The authors believe that even if a person is being photographed (filmed) in a public place, but shows clear disagreement of that, such filming should be discontinued, as the person in public places does not loose the protection of his/her privacy. Such attitude corresponds with and is based on Lithuanian case law which says that «*a person even being in a public place, does not loose his/her individuality and privacy, therefore a subjective inner possition of a person photographed is important; if such person clearly and unambiguously expresses his/her unwillingness to be photographed, it must be respected*».[3] Under current Lithuanian regulation, to be more precise, lack of regulation, to express unwillingness to be photographed (filmed) by usage of a dashboard camera or UAS is impossible as the person filmed in most of the cases does not even know about it. Thus, using dasboard cameras without special marking informing others about filming, equates to secret filming, therefore it takes away the opportunity to express clear disagreement with the ongoing process. Furthermore, even special marking does not prevent from privacy breaches (breaches of a person's right to an image), as the person filmed, even noticing the marked car, could not have a chance to express his/her disagreement (for example, if the car is moving fast). Therefore, stricter regulation on the usage of footage is essential (for example, clear prohibition to make public videos, taken by dashboard cameras, in which private information (for example, car number plates) or people's faces could be seen, except for reasons, such as public interest, disclosure of violations of the law.

[1] Ibid: 6.246, 6.247, 6.248.

[2] Ibid: 2.22.

[3] *J. A., UAB „Lietuvos rytas"*. Ruling of the Supreme Court of Lithuania, 2004, No. 3K-3-91/2004.

Protection of privacy is enshrined in Lithuanian administrative and criminal law. However, the code of administrative offences sets the fines only for unauthorized processing of personal data and privacy breach in the area of electronic communications (applied for activities of entities, providing or entitled to provide a public communications network or related facilities only[1]) and for the breaches of LPDLP[2], which also applies to business entities only. However, the code also sets the prohibition to breach The rules for the use of unmanned aircrafts.[3] Even though, as it was mentioned earlier, they are designed to regulate questions of security on the usage of UAS, at the same time this administrative tool could be used to defend interests of privacy subjects (if noticed that the UAS is being flown over private area and requirements of distance, location are breached, the injured person on the grounds of these rules could request for stopping the UAS monitoring activities).

Section XXIV of the Criminal Code of the Republic of Lithuania sets the crimes related to inviolability of private life. Among the crimes mentioned there are articles criminalizing trespass,[4] illegal collection of information about a person's private life and making available to the public,[5] exploitation, or exploitation for the benefit of third parties information about someone's private life without his consent if this information was received for the accused person's service, profession or during the performance of temporary task, or by committing one of the crimes named above[6]. However, because none of these crimes are classified as the crimes for negligent commitment of which the prosecution is allowed, in order to arraign on earlier mentioned crime charges, direct intention to commit a crime must be proven.[7] Thus, in case of the usage of the image capturing devices analysed, it would be very difficult to prove direct intention of the breacher of the right to privacy.

It is obvious that «*privacy is a culture-specific: the matters which a particular society regards as 'private' can vary widely*».[8] Even very gerographically, historically and culturally close countries, could have quite a different regulation on privacy and its protection. For example, even though the privacy in Latvia is also protected by the legal act of supreme power – the Constitution[9], but the most detailed regulation

[1] Elektroninių ryљių įstatymas (Law on Electronic Communications). Official Gazette, 2004, No. 69-2382: 32; Lietuvos Respublikos administracinių nusižengimų kodeksas (Code of Administrative Offences of the Republic of Lithuania). TAR, 2015, no. 2015-11216: 83.

[2] Lietuvos Respublikos administracinių nusižengimų kodeksas(ibid): 82.

[3] Ibid: 393(2).

[4] Lietuvos Respublikos baudžiamasis kodeksas (Criminal Code of the Republic of Lithuania). Official Gazette, 2000, No. 89-2741: 165.

[5] Ibid: 167.

[6] Ibid: 168.

[7] Ibid: 16(4) („A person shall be punishable for commission of a crime or misdemeanour through negligence solely in the cases provided for separately in the Special Part of this Code"). See also *S.B., V.B., R.B.* Ruling of Taurage District Court, 2011, No. PK-72-635/2011;

[8] Requoted from Michael, J. (1994). *Privacy and Human Rights: International and Comparative Study, with Special Reference to developments information technology.* Dartmouth: Unesco Publishing: 2.

[9] Constitution of the Republic of Latvia, Adopted on 15.02.1922. Published: Latvijas Vestnesis, 01/07, 13.06.43. Last amendments 08.04.2009: 96: „Everyone has the right to inviolability of his or her private life, home and correspondence"

on personal data protection in Latvia is set in the recent Personal Data Processing Law[1], which since 5th July 2018 replaced Personal Data Protection Law.[2] Its predecessor, contrary to Lithuanian situation, did not set any special conditions under the existence of which precisely video surveillance was allowed (only paragraph 7 obliged to make sure that at least one of the six conditions exists in order to generally process personal data). Whereas in the new Latvian law – Personal Data Processing Law, separate article is dedicated precisely to the conditions of video surveillance (and especially carried out by dashboard cameras) and it says that «*The requirements of this Law and the Data Regulation do not apply to the processing of data by natural persons using automated data recording devices for road traffic, personal or household needs.*» In the same article it is also stressed that «*It is prohibited to disclose the records obtained in road traffic to other persons and institutions, except when one of the bases of data processing specified in the data regulation is found. The requirements of this Law and the Data Regulation do not apply to the processing of data by natural persons using automated video surveillance devices for personal or household use.*»[3] Thus, the provision does not only set the rules on video surveillance in traffic (that it is forbidden to disclose the records), but also confirms the specificity of dashboard cameras as a data collection device. What is interesting that even though Latvian laws, on the contrary to Lithuanian, do not distinguish person's right to an image (including his/her right to expressively dissagree of being filmed), but, again, on the contrary to Lithuaniam regulation, they clearly state that records obtained by dashboard cameras cannot be disclosed to other persons and institutions (except for separately indicated cases).[4] Furthermore, the same article also states that it is prohibited to disclose the records obtained in road traffic to other persons and institutions, except when one of the bases of data processing specified in the data regulation is found (see GDPR Article 6(1)), whereas Lithuanian Civil Code does not protect privacy subjects from their images, taken in public, being demonstrated publicly if they do not harm the subjects' reputation, honor, dignity.[5] Thus, if a dashboard camera recorded a video in which a person could be recognized and this video was made public, under Lithuanian law, no offence is made, as the dignity, honor and reputation of the person in the video has not been breached. So, it could be said that the person was filmed without even knowing it and without being able to express his disagreement with the process despite the fact that he or she did not want to be recognized as being in particular place at the particular time or driving a/sitting in a particular car.

Furthermore, Latvian civil code, on the contrary to Lithaunian, does not govern privacy questions at all. However, abundance of privacy-protecting articles in

[1] Personal Data Processing Law. Published: Latvijas Vēstnesis , 04.07.2018, 132 (6218), available at: https://likumi.lv/ta/id/300099-fizisko-personu-datu-apstrades-likums.

[2] Personal Data Protection Law. Published: Latvijas Vēstnesis, 06.04.2000, 123/124 (2034/2035), «The Reporter», 9, May 4, 2000, available at: https://likumi.lv/ta/id/4042-fizisko-personu-datu-aizsardzibas-likums.

[3] Personal Data Processing Law, supra note 44: 36.

[4] Ibid: 36(2).

[5] Civil Code of the Republic of Lithuania, supra note 31: 2.22 (2).

administrative and criminal codes proves legislator's responsible attitude towards privacy. For example, Administrative violations' code of Latvia sets the offences connected with the breaches of private life and applicable in the usage of image capturing devices (illegal activities with personal data (including data collection, registration, entry, storage, arrangement, modification, use, transfer, transmission, disclosure, blocking or deletion),[1] failure to provide information to the data subject,[2] processing of personal data without registration[3]. Furthermore, if these articles are not sufficient to protect natural person from his privacy breaches commited by usage of image capturing devices, other articles, punishing the offender for the breaches of usage of, for example, UAS, could be used (for example, Article 114[1]). However, it is important to stress that the disposition of this article describes only activities connected with aircrafts, whereas UAS under the national rules on UAS usage («Procedures for the Conduct of Unmanned Aerial Vehicles and Other Types of Aircraft which do not Classify as Aircraft» (hereinafter – UA Rules),[4] are not treated as aircrafts.[5] However, as there are no any specific article connected with the breaches of this article is being used by analogy. Besides, the right to privacy which could be breached by the usage of image capturing devices, is also protected by the Criminal Law of Latvia, which criminalizes violation of the privacy of a person[6] and illegal activities with personal data.[7] It is important to stress that Latvian case law and scholars have not yet confirmed that entering a private territory with the help of a device (for example UAS) is the breach of person's privacy, therefore it is still treated that the person himself/hereself has to enter the private territory in order to commit a crime.[8]

Even though Latvia, as well as Lithuania, does not have separate regulation on the usage of dashboard cameras, but it also has special regulation on the usage of UAS (UA Rules). On the contrary to Lithuanian Rules, UA Rules at least mention the respect for privacy in the course of usage of the UAS: «*Unmanned aircraft flights shall be performed so as not to endanger human life, health, privacy or property, flight safety and security, not to cause harm to the environment, and also not to endanger the State defence and security interests*»,[9] but no further special privacy protection

[1] Code of Administrative Violations of the Republic of Latvia. Published: Reporters, 20.12.1984, 51, available at: https://likumi.lv/ta/id/89648-latvijas-administrativo-parkapumu-kodekss: 204-7

[2] Ibid: 204-8.

[3] Ibid: 204-9.

[4] Procedures for the Conduct of Unmanned Aerial Vehicles and Other Types of Aircraft which do not Classify as Aircraft. Adopted on 22.11.2016. Published: Latvijas Vestnesis, 28.11.2016, 231 (5803), available at: https://likumi.lv/ta/id/286823-kartiba-kada-veicami-bezpilota-gaisa-kugu-un-tadu-cita-veida-lidaparatu-lidojumi-kuri-nav-kvalificejami-ka-gaisa-kugi.

[5] Ibid: 1.

[6] Criminal Law. Published: Latvijas Vēstnesis, 08.07.1998, 199/200 (1260/1261), «The Reporter», 04.08.1998, 15, available at: https://likumi.lv/doc.php?id=88966: 143.

[7] Ibid: 145.

[8] Krastiņļ, U., Liholaja, V. (2016). *Krimināllikuma komentāri. Otrā daļa (IX-XVII nodaļa)*. Rīga: Tiesu namu aģentūra, pp 341, 352.

[9] Procedures for the Conduct of Unmanned Aerial Vehicles and Other Types of Aircraft which do not Classify as Aircraft, supra note 52: 8.

provisions could be found in this act. However, it is important to stress that, on the contrary to Lithuanian Rules, UA Rules contain provisions obliging the owner of the UAS to label the device with the given name and surname (for legal persons – company name) of the owner or possessor thereof, address of the declared place of residence (for legal persons – legal address) and phone number.[1] This obligation corresponds with the recommendations set in the Regulation EU 2018/1139 (as it was mentioned earlier – to make sure that the UAS is identifiable).[2] Also, the UA rules oblige the pilot of unmanned aircraft be identifiable.[3] These requirements ensure easy determination and identification of the person managing the UAS in cases when there is a question of any kind of liability and in such way serve not only for safety ensurance but for privacy protection as well (when the responsible person concerning privacy breaches must be found or illegal obserevation of private areas has to be interrupted). These requirements are useful and practical steps towards realistic, not only formal, implementation of privacy protection. However, modeling situation that a person breaches the requirements of the device and self identification assuranace, it would still be very hard to identify the offender (in case of privacy breaches when using UAS).

As it was mentioned earlier, netiher Lithuania has special regulation, nor Latvia has detailed regulation on dashboard cameras' use and even though there are plenty of rules concerning privacy protection in criminal, administrative law acts, as well as in civil ones (in Lithuania), but if it is impossible to identify the offender of someone's privacy, all these acts are vain. So, in order to ensure the identification of a manager of an image capturing device, besides obligations enshrined in Latvian UA rules (to make sure the device and its operator are identifiable) it is also recommended to oblige to appropriately mark cars (for example, with camera signs and driver's contact details) in which dashboard cameras are used so that other road users are informed about personal data being collected. If determined that no appropriate marking is used, administrative fines must be set.

As it was noticed, Lithuanian and Latvian legislation on privacy protection differs: in the Lithuanian legislation on the usage of UAS there is a lack of rules actually ensuring the protection of privacy. The same problem is with dashboard cameras in both countries compared: none of them sets the requirement to specifically mark the cars in which dashboard camera is being used, therefore neither the dashboard camera users are motivated to act in such a manner that other people's privacy is respected (for example, knowing that others are informed about a dashboard camera being used, its user is more motivated to act in a propper manner), nor potential injured persons can protect themselves from being filmed or know to

[1] Procedures for the Conduct of Unmanned Aerial Vehicles and Other Types of Aircraft which do not Classify as Aircraft, supra note 52: 8.

[2] EU, "Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency ", supra note 31: Anex IX, p. 1.3.

[3] Procedures for the Conduct of Unmanned Aerial Vehicles and Other Types of Aircraft which do not Classify as Aircraft, supra note 52: 28.

whom express their disagreement to be filmed; Latvian criminal law (or case law) has not yet reflected the development of technologies and the threat they could cause, therefore watching private territories with UAS is not treated as transgression of inviolability of the apartment of a person. Thus, if a person in Lithuania could defend his/her privacy on the basis of Civil code which protects person's right to privacy, in Latvia the injured person could invoke criminal and administrative laws only (as Latvian Civil law does not contain provisions neither on privacy protection nor on people's right to an image).

The protection of personal data, as a part of the right to privacy, is very important and as stated in the preamble of the GDPR is officially treated as the fundamental one.[1] However, the authors of this article agree with professor David Flaherty who has stated that the right to privacy «is not identical to such fundamental values as liberty, freedom, and democracy».[2] This could also be confirmed by the rulings of European Court of Human Rights which allowed for certain limitations by stating that it would be too restrictive to limit the notion of «private life» to an «inner circle» in which the individual may live his or her own personal life as he or she chooses, thus excluding entirely the outside world not encompassed within that circle.[3] So, no legal act can protect people's privacy in such a manner that particular individual is totally protected from outside world. In such case whatever threatens privacy, would have to be forbidden. But on the other hand, the limitations of the protection of privacy have to be reasonable. Thus, even though the European Court of Human Rights has explained that «the notion of 'private life' within the meaning of Article 8 of the Convention is a broad concept...,»[4] which «is not susceptible to exhaustive definition»[5], but it is definitely connected with various rights, such as the right to personal development,[6] right of living privately, away from unwanted attention[7] and these rights are protected if a reasonable expectation that their privacy would be respected exists.[8]

Furthermore, similar flexible attitude to the right to privacy is reflected in the Euroepan Union legislation. For example, in the preamble of the GDPR it is stated that «*The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality*.»[9]

So, as the use of UAS and dashboard cameras cannot be denied and the fact that the right to privacy is not absolute has been supported by the examples above,

[1] General Data Protection Regulation, supra note 1: 2.
[2] Flaherty, D.H. (1984). *Privacy and Data Protection: An International Bibliography,* London: Mansell.
[3] *Niemietz v. Germany*, December 16, 1992, § 29, Series A no. 251-B.
[4] M.M. v. Russia, no. 7653/06, ECHR 1237
[5] *Sargsyan v. Azerbaijan [GC]*, no. 40167/06, § 255, ECHR 2015; *Sidabras and Džiautas v. Lithuania*, nos. 55480/00 and 59330/00, § 43, ECHR 2004-VIII.
[6] *K.A. and A.D. v. Belgium*, nos. 42758/98 and 45558/99, § 83, February 17, 2005
[7] *Smirnova v. Russia*, nos. 46133/99 and 48183/99, § 95, ECHR 2003-IX (extracts).
[8] *Köpke v. Germany (dec.)*, no. 420/07, October 5, 2010
[9] General Data protection Regulation, supra note 1: 4.

it is important to specify, what assures the achievement of the societal security and privacy balance.

2.2. Tackling illegal usage of image capturing devices

The most realistic and the most effective way of protecting subcets of privacy is threatening legal responsibility for the breaches of people's privacy and clear and effective rules of the usage of image capturing devices. Such responsibility, as it was seen before, under national laws could be criminal, administrative and civil. After a concise review of Lithuanian and Latvian national legislations, it is obvious, that both countries made a great job in reconciling GDPR with their national laws. However, as Personal Data Processing Law and LPDLP set the requirements for data processing by business entities or natural persons (for business purposes), it is obvious, that the biggest threat to people's privacy are private users of image capturing devices, which do not fall under the provisions of the GDPR and, accordingly, Personal Data Processing Law (in Latvia) and LPDLP (in Lithuania). First of all, there is a lack of clear obligation for all users (including private ones) to mark themselves and their devices (UAS and cars in which dashboard cameras are used) (only Latvian legislation has moved forward in obliging such users to make themselves identifiable when operating UAS, but such obligation does not exist in regard to dashboard camera usage in both countries, therefore the cars in which dashboard cameras are used should also be marked with a special sign and contact details of the user). Furthermore, when clear obligation for the operators of image capturing devices to identify themselves and their devices being operated is fulfilled, the subjects of private information have to have possibility to express their disagreement with the action (as in Lithuania: the case law has formulated the provision that a clear expression of disagreement (verbal or non-verbal) prohibits the disclosure of information collected). Taking into consideration specificity of dashboard cameras (that even if a subject of private information is informed about the private information being collected (in other words, about video surveillance being carried out) but the right of disagreement with the operation could be hardly implemented as the cars move fast and in a traffic flow the subjects of private information may not even notice that they are being filmed), a clear prohibition for natural persons to use records or make them public taken by dashboard cameras must exist (with exceptions of public interest, and help to reveal the circumstances of various violations – to courts, preliminary investigation institutions or police).

Furthermore, it is worth considering the fact that the UAS or dashboard camera could be used by natural persons for various illegal purposes, such as spying. So, the video taken shall not be made public, but the operator will achieve his/her unlawful goal at the same infringing someone's right to privacy. In such situation the injured person will not have a chance of proving that he/she was being spied on. Therefore administrative national acts on the usage of UAS must strictly forbid using the devices in residential neighbourhoods and above private territories[1] and for such breaches strict administrative fines must be set.

[1] The Rules do not contain prohibition to fly over a private territory if it is not in a town, city or densely populated area.

Conclusions. After the comparison of two legislations governing the same questions of privacy and usage of UAS and dashboard cameras, it is clear that national laws, even both being in accordance with one – European Union legislation – could protect the same value with different legal tools. Each legislation – Lithuanian and Latvian – has its own advantages and disadvantages, but what could be confirmed is that the law does not always go in step with the quick development of technologies. As it has been seen, with particular adjustments concerning identification of the users of UAS and dashboard cameras, with introduction of legal tools allowing the injured party to efficiently defend their privacy in cases when the personal information users are persons gathering someone's private information for non-commercial purposes, the right balance between the two values – societal security and privacy – could be found.

The advantages of the new technologies could not be denied, therefore it would be absurd to say that they are not necessary as causing to much danger to our privacy. And privacy as a value could not be absolute. Therefore it is essential to adapt legal mechanisms to the changing threats to the main values, such as privacy. Thus, the lack of legal measures could not be the reason to interfere with technological development: not the new technologies should be treated as a threat, but legal norms should be improved and adjusted to the constantly changing world.

References:

1. Bučiūnas, G. (2015). Vaizdo registratoriai ir asmens privatumas, *Mokslo taikomieji tyrimai Lietuvos kolegijose*, Vol. 1, No. 11, pp. 64–68.

2. Dupont, Q. F. M., Chua, D. K.H., Tashrif, A., Abbott, E. L.S. (2017). Potential Applications of UAV along the Contruction's Value Chain, *Procedia Engineering*, Vol. 182, pp. 165–173.

3. Entrop, A.G., Vasenev, A. (2017). Infrared Drones in the Construction Industry: Designing a Protocol for Building Thermography Procedures, *Energy Procedia*, Vol. 132, pp. 63–68.

4. EU Open Data Portal, «Special Eurobarometer 432: Europeans' attitudes towards security». (2015). Retrieved 25.11.2017 from http://data.europa.eu/euodp/en/data/dataset/S2085_83_2_432_ENG/resource/ae0b54bc-3974-4165-9f7d-c2907cb3f41f.

5. European Commission, Retrieved 15.07.2018 from https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en.

6. Flaherty, D.H. (1984). *Privacy and Data Protection: An International Bibliography*, London: Mansell, 302 p.

7. Hertz, L.H. (1967). *The Complete Book of Model Aircraft Spacecraft and Rockets*, Crown Publishers, 278 p.

8. Joseph J. Vacek, J.J. (2014). Remote Sensing of Private Data By Drone sis Mostly Unregulated: Reasonable Expectations Of Privacy Are at Risk Absent Comprehensive Federal Legislation, *North Dakota Law Review*, Vol. 90:463–484.

9. Kavoosi, Z., Hossein Raoufat, M., Dehghaani, M., Jafari, A., Kazemeini, A., Jafar Naazemossadat, M., (2018). Feasibility of satellite and drone images for monitoring soil residue cover, *Journal of the Saudi Society of Agricultural Sciences*, «in press» version doi: https://doi.org/10.1016/j.jssas.2018.06.001.

10. Khan, M. A., Ectors, W., Bellemans, T., Ruichek, Y., Yasar, A. H., Janssens, D., Wets, G. (2018). Unmanned Aerial-Vehicle Based Traffic Analysis: A Case Study to Analyze Traffic Streams at Urban Roundabouts, *Procedia Computer Science*, Vol. 130, pp 636–643.

11. Krastiņš, U., Liholaja, V. (2016). *Krimināllikuma komentāri. Otrā daļa (IX–XVII nodaļa)*. Rīga: Tiesu namu aģentūra, 512 p.

12. McKown, M (2015). The New Drone State: Suggestions for Legislatures Seeking to Limit Drone Surveillance by Government and Nongovernment Controllers, *University of Florida Journal of Law and Public Policy, vol.* 26, pp. 71–90.

13. Michael, J. (1994). *Privacy and Human Rights: International and Comparative Study, with Special Reference to developments information technology*. Dartmouth: Unesco Publishin, 194 p.

14. Nauwelaerts, W., World Data Protection Report: Guidelines on Use of Dashboard Cameras (2014), retrieved 06.05.2018 from https://www.hunton.com/files/Publication/a75c66a4-2f6f-4e3e-a83b-543923987393/Presentation/PublicationAttachment/580a5a0c-66f6-4cee-834c-8b41b637fd09/Guidelines_on_Use_of_Dashboard_Cameras.pdf.

15. Puraite, A., Bereikiene D., Silinske, N. (2017). Regulation of Unmanned Aerial Systems and Related Privacy Issues in Lithuania, *Baltic Journal of Law and Politics*, Vol. 10:2, pp. 107–132.

16. Puraite, A., Silinske, N. (2017). Understanding the concept of security: theoretical approach. *Public Security and Public Order*, Vol. 19, pp. 135–145.

17. Rogavichene, L., Garmonnikov, I. (2017). Innovative Technologies for Assessment and Correction of the Driving Style, *Transportation Research Procedia*, Vol. 20, pp. 564–570.

18. SESAR, European Dornes Outlook Study, Retrieved 01.02.2018 from https://www.sesarju.eu/sites/default/files/documents/reports/European_Drones_Outlook_Study_2016.pdf, 93 p.

19. The Telegraph, retreived 06.05.2018 from https://www.telegraph.co.uk/business/risk-insights/dashcam-benefits/.

20. Vadapalas, V. (1998). *Tarptautinė teisė. Bendroji dalis (International Law. General Part)*, Vilnius: Eugrimas, 371 p.

21. Villasenor, J. (2013). Observation from above: Unmaneed Aircraft Systems and Privacy. *Harvard Journal of Law and Public Policy*, Vol 36, pp 457-517.

Legal references:

22. *Amann v. Switzerland*, No. 27798/95, ECHR 2000-II.

23. *Asmens duomenų teisinės apsaugos įstatymas (Law on Personal Data Legal Protection)*. Official Gazette, latest amendment 2008, no. 22–804.

24. *Bepiločių orlaivių naudojimo taisyklės (The rules for the use of unmanned aircrafts)*. TAR, 2014, No. 2014-00438.

25. Charter of Fundamental Rights of the European Union, 7.12.2000, OJ C 326, 26.10.2012, *p*p. 391–407.

26. Code of Administrative Violations of the Republic of Latvia. Published: Reporters, 20.12.1984, 51, available at: https://likumi.lv/ta/id/89648-latvijas-administrativo-parkapumu-kodekss.

27. Constitution of the Republic of Latvia, Adopted on 15.02.1922. Published: Latvijas Vestnesis, 01/07, 13.06.43. Last amendments 08.04.2009.

28. Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14. 1950, ETS 5, available at: http://www.refworld.org/docid/3ae6b3b04.html.

29. Criminal Law. Published: Latvijas Vēstnesis, 08.07.1998, 199/200 (1260/1261), «The Reporter», 04.08.1998, 15, available at: https://likumi.lv/doc.php?id=88966.

30. Elektroninių ryљių įstatymas (Law on Electronic Communications). Official Gazette, 2004, No. 69–2382.

31. Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 (Text with EEA relevance.), *OJ L 212, 22.8.2018, pp. 1–122*.

32. *J. A., UAB «Lietuvos rytas»*. Ruling of the Supreme Court of Lithuania, 2004, No. 3K-3-91/2004.

33. *K.A. and A.D. v. Belgium*, nos. 42758/98 and 45558/99, § 83, February 17, 2005.

34. *Kupke v. Germany (dec.)*, no. 420/07, October 5, 2010.

35. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas (Law on Personal Data Legal Protection of the Republic of Lithuania), Official Gazette, 1996, No. 63–1479; 2000, No. 64–1924; 2003, No. 15–597; 2008, No. 22–804; TAR, 2018-07-11, No. 2018–11733.

36. Lietuvos Respublikos administracinių nusižengimų kodeksas (Code of Administrative Offences of the Republic of Lithuania). TAR, 2015, No. 2015–11216.

37. Lietuvos Respublikos baudžiamasis kodeksas (Criminal Code of the Republic of Lithuania). Official Gazette, 2000, No. 89–2741.

38. Lietuvos Respublikos civilinis kodeksas (Civil Code of the Republic of Lithuania). Official Gazette, 2000, no. 74–2262; 200.

39. *Lietuvos Respublikos Konstitucija (Constitution of the Republic of Lithuania)*, Official Gazette (1992, no. 220, 33–1014).

40. *M.M. v. Russia*, no. 7653/06, ECHR 1237.

41. *Niemietz v. Germany*, December 16, 1992, § 29, Series A no. 251-B.

42. Personal Data Processing Law. Published: Latvijas Vēstnesis , 04.07.2018, 132 (6218), available at: https://likumi.lv/ta/id/300099-fizisko-personu-datu-apstrades-likums.

43. Personal Data Protection Act, Estonia, Isikuandmete kaitse seadus, adopted on 15.02.2007, RT I 2007, 24, 127, available at: https://www.riigiteataja.ee/en/eli/ee/507032016001/consolide/current.

44. Personal Data Protection Law. Published: Latvijas Vēstnesis, 06.04.2000, 123/124 (2034/2035), «The Reporter», 9, May 4, 2000, available at: https://likumi.lv/ta/id/4042-fizisko-personu-datu-aizsardzibas-likums.

45. Procedures for the Conduct of Unmanned Aerial Vehicles and Other Types of Aircraft which do not Classify as Aircraft. Adopted on 22.11.2016. Published: Latvijas Vestnesis, 28.11.2016, 231 (5803), available at: https://likumi.lv/ta/id/286823-kartiba-kada-veicami-bezpilota-gaisa-kugu-untadu-cita-veida-lidaparatu-lidojumi-kuri-nav-kvalificejami-ka-gaisa-kugi.

46. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *OJ L 119, 4.5.2016*.

47. Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 (Text with EEA relevance.), *OJ L 212, 22.8.2018, pp. 1–122*.

48. *Sargsyan v. Azerbaijan [GC]*, no. 40167/06, § 255, ECHR 2015.

49. *S.B., V.B., R.B.* Ruling of Taurage District Court, 2011, No. PK-72-635/2011.

50. *Sidabras and Džiautas v. Lithuania*, nos. 55480/00 and 59330/00, § 43, ECHR 2004-VIII.

51. *Smirnova v. Russia*, nos. 46133/99 and 48183/99, § 95, ECHR 2003-IX (extracts).

52. Universal Declaration of Human Rights, 1948, Paris. Retrieved from: http://www.un.org/en/universal-declaration-human-rights/.

Пурайте А., доцент, факультет общественной безопасности, Университет Миколаса Ромериса, Литовская Республика, г. Каунас.

e-mail : aurelija.puraite@gmail.com

Силинску Н., аспирантка, факультет права, Университет Туриба, Латвия, г. Рига.

e-mail : n.silinske@gmail.com

Приборы, фиксирующие изображения: угроза или благо?

Авторы статьи «взвесили» преимущества и угрозы вмешательства в частную жизнь, возникающие в результате использования беспилотных летательных аппаратов (дронов) и видеорегистратора. Анализируя и сравнивая законодательство двух географически, исторически и культурно близких стран – Латвии и Литвы, они указывают на различия в законодательном урегулировании вопросов конфиденциальности, проблемные аспекты их действующего национального законодательства по использованию технологий и защите частной жизни, а также предлагают возможные решения по урегулированию выявленных правовых пробелов.

Ключевые слова: беспилотные летательные аппараты; дроны; видеорегистраторы; собственность; Латвия; Литовская Республика.

Рекомендоване цитування: Pūraitė A., Šilinskė N. Image capturing devices: threat or good? *Проблеми законності*. 2019. Вип. 144. С. 120–137. doi: https://doi.org/10.21564/2414-990x.144.157226.

Suggested Citation: Pūraitė, A., Šilinskė, N. (2019). Image capturing devices: threat or good? *Problemy zakonnosti – Problems of Legality, issue 144, 120–137*. doi: https://doi.org/10.21564/2414-990x.144.157226.

Надійшла до редколегії 09.01.2019 р.